10TH INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM
The Future of C2

"Are Service Oriented Architectures the Only Valid Architectural Approach for the Transformation to Network Centric Warfare?"

Topic: C4ISR Architecture
Date: June 2004
Presenter & Author: Jack Lenahan
Imagine-One Corporation
Office of The Chief Engineer
Space and NAVAL Warfare Systems Center
Charleston, South Carolina
Contact Information
Email – John.Lenahan@Navy.mil
Phone – 843-218-6080

1. REPORT DATE **JUN 2005**	2. REPORT TYPE	3. DATES COVERED **00-00-2005 to 00-00-2005**
4. TITLE AND SUBTITLE **Are Service Oriented Architectures the Only Valid Architectural Approach for the Transformation to Network Centric Warfare? (Briefing Charts)**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Space and Naval Warfare Systems Center,PO Box 190022,North Charleston,SC,29419-9022**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release; distribution unlimited**		
13. SUPPLEMENTARY NOTES **The original document contains color images.**		
14. ABSTRACT		
15. SUBJECT TERMS		

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES **12**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

<u>Agenda</u>

- **The issue addressed**
- **What are the basic NCW Infrastructure Architectural Requirements?**
  - **Reliability**
  - **Availability**
  - **Scalability**
- **What is an SOA?**
  - **Software Architecture**
    - **Highly Available (HA) Software Stack**
    - **HA + Disaster Recoverable (DR) Software Stack**
  - **Hardware Architecture**
- **What are other alternatives?**
  - **MOMS**
  - **GRIDS**
  - **EDA**
- **Quality of Service Architecture Rating Scale**
- **Conclusion**
  - **What solution meets the architectural requirements?**
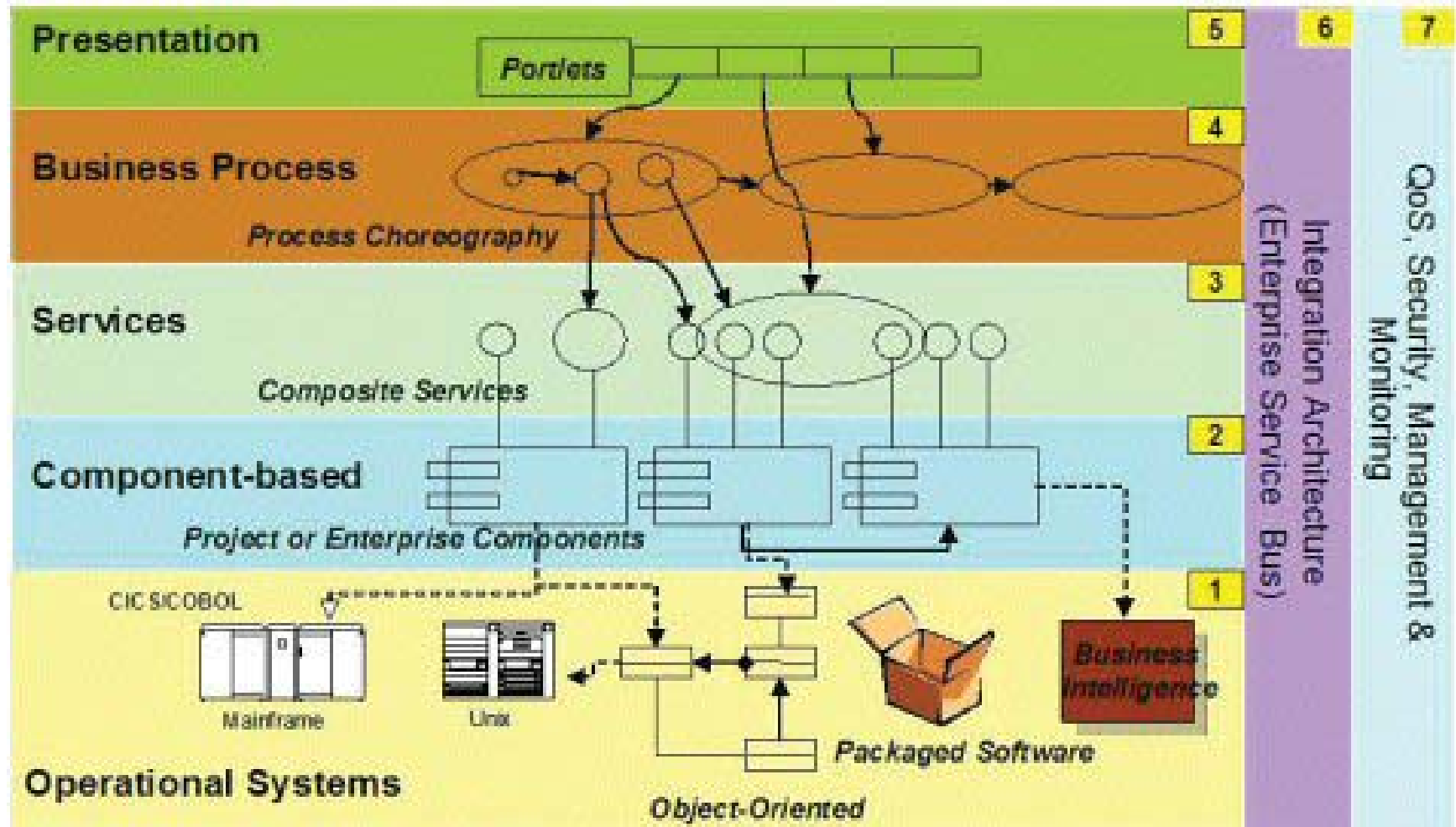 - **What does it look like?**

Issue Addressed

The use of a Service Oriented Architecture (SOA) as the dominant single architectural design paradigm of Network Centric Warfare (NCW) introduces architectural infrastructure stability risk levels which may be unacceptable in C4ISR mission frameworks.
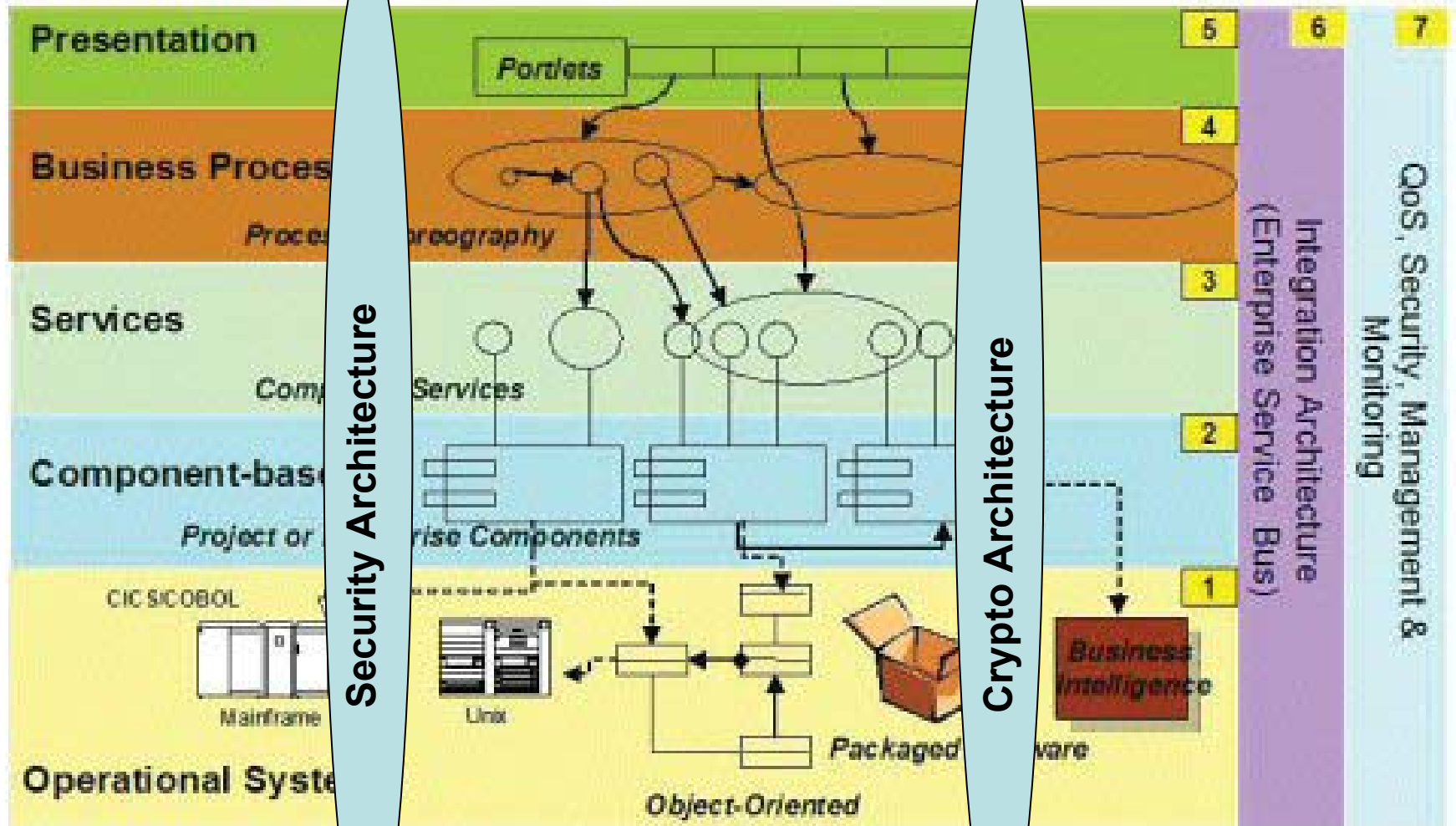
Infrastructure Requirements

- **Reliability** - *SOA software vendors must deliver software which will not fail between the start of the mission and the end of the mission regardless of mission duration.*

- **Availability** – 5 nines - *any component exceeding unavailability of 1.44 minutes per day violates quality of service at any level But this is in addition to and does not replace the primary availability requirement that no failures visible to the user can be tolerated during combat missions.*

- **Performance** - *The performance requirement is that no service can degrade below a pre-defined (hopefully tagged) SLA/QoS performance threshold. Performance must be monitored and if degradation is detected, re-routing of the service must occur transparent to the user.*

- ***No single points of failure can be tolerated in the hardware or software architecture stacks***

Software Architecture Layers

Software Architecture Layers

Presentation — 5 — 6 — 7

Portlets

Business Process — 4

Process Choreography

Services — 3

Composite Services

Component-based — 2

Project or Enterprise Components

CIC SICOBOL

Mainframe

Units

Operational System — 1

Object-Oriented

Packaged Software

Business Intelligence

Integration Architecture (Enterprise Service Bus)

QoS, Security, Management & Monitoring

Security Architecture

Crypto Architecture

Highly Available Software Stacks

Full HA at All SW Layers – No DR
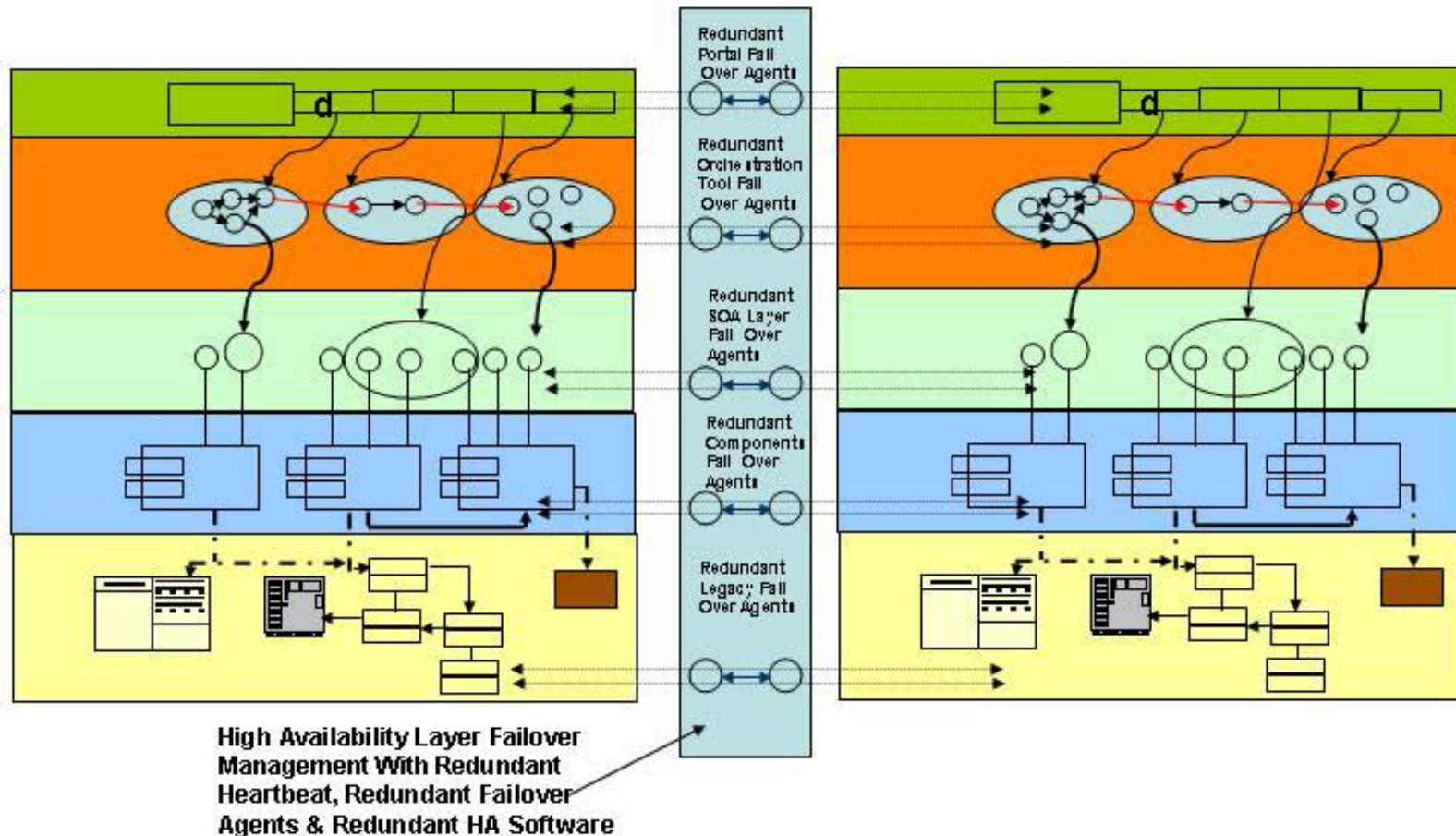
Highly Available – Disaster Recoverable Software Stacks

Full HA – With DR

Disaster Recovery
Management Layer -
Redundant Disaster State
Monitoring Agents &
Heartbeat Paths

High Availability Management Layers -
Failover Management with Redundant
Heartbeat & Redundant HA Agents &
Software

DR Capabilities
Physically Removed
From HA Locations
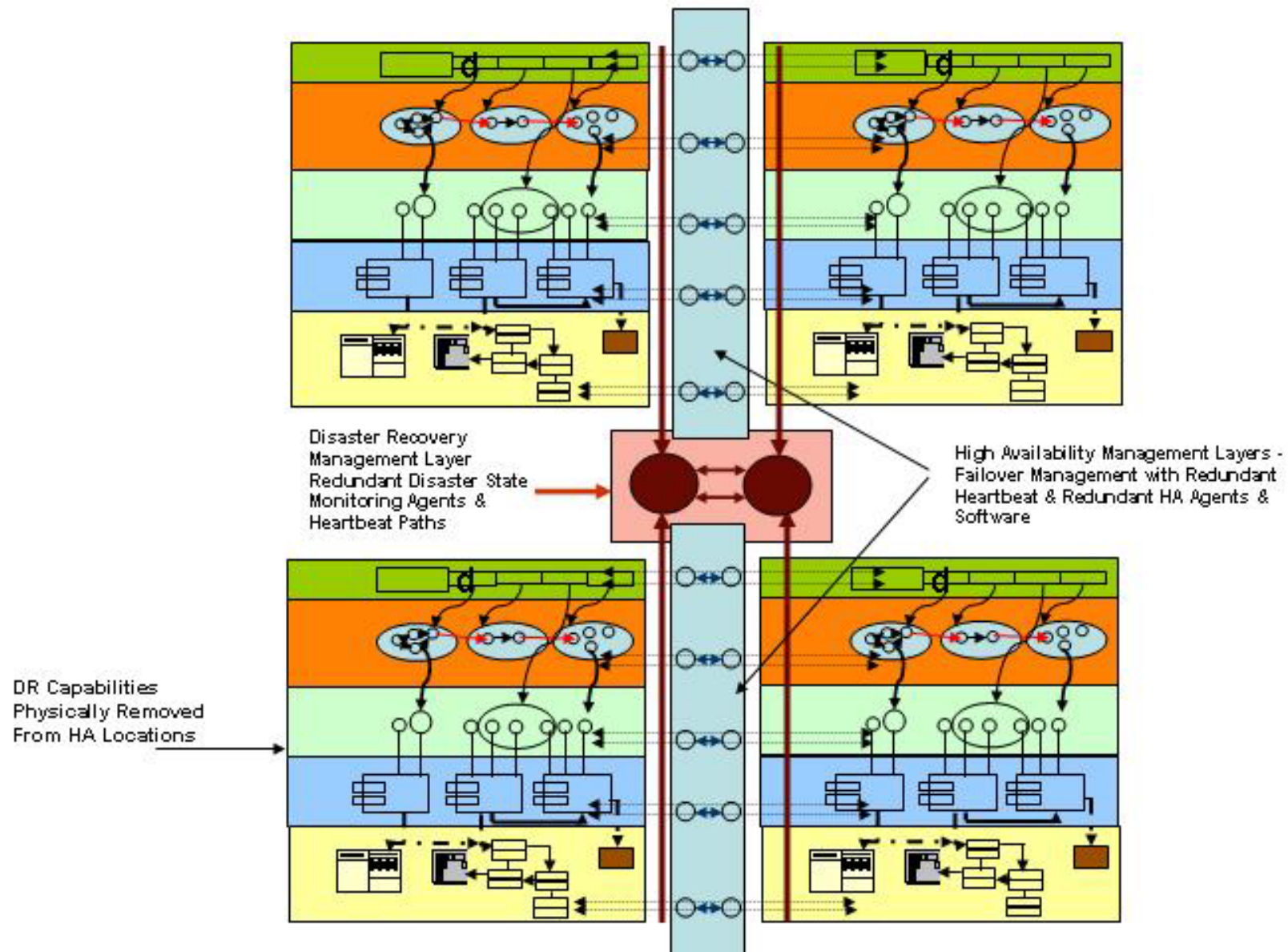
Hardware Architecture

The 13.6 TF TeraGrid:
Computing at 40 Gb/s
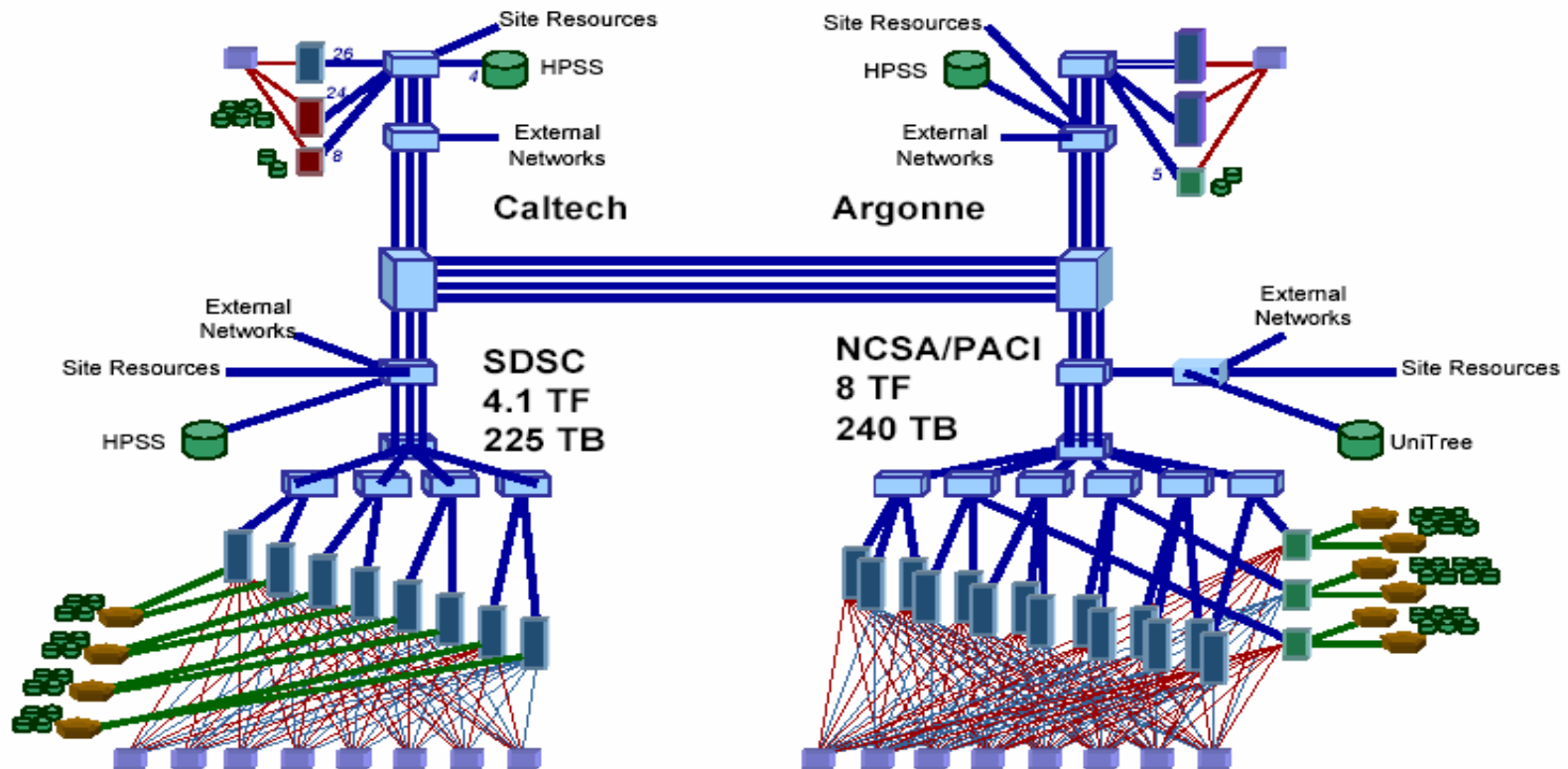
NCSA, SDSC, Caltech, Argonne   www.teragrid.org

**GRID Architecture – A Complex Adaptive System which
is scaleable, highly available, disaster recoverable, and capable
of dynamic program execution resource re-assignment.**

Lenahan Levels of NCW Architectural QoS for Web Services Implementations

QoS Level	Capability or Capability Sets exposed as Web Services	State Recording	Simple State Recording with graceful fail over management by simple agents	Agent Monitoring of All Web Services in given C4ISR Architectural Orchestration or Choreography for Graceful Recovery of Services (Also applies to each service and its orchestration tool in a given FNEP being fully Stateful and agent monitored)	HA (All enabling software / hardware infrastructure layers (Listeners, Authentication SW, Firewalls, Single Sign-on Software, Directory and Naming Management, MOMS, Database Software, Redundant Directories, Redundant data, SAN, NIC, etc) for the entire orchestration set)	HA with Full DR - Clone Of HA Suites	HA/DR with guaranteed performance management (GRIDS Only with all 7 ISO Layers HA/DR)
1	Y	N	N	N	N	N	N
2	Y	Y	N	N	N	N	N
3	Y	Y	Y	N	N	N	N
4	Y	Y	Y	Y	N	N	N
5	Y	Y	Y	Y	Y	N	N
6	Y	Y	Y	Y	Y	Y	N
7	Y	Y	Y	Y	Y	Y	Y

Conclusion & Recommendation

- **Summary of The Analysis:**
  - **That all levels of the model, including the communications and networking not depicted, must be highly available to support 5 nines availability, (one set of clones) and disaster recoverable (a second set of clones)**
  - **That all tools embedded in the SOA (particularly the choreography, orchestration, and single-sign-on software) must also be redundant**
  - **The HA/DR monitoring agents themselves must be HA/DR**
  - **Increased use due to new conflicts or surge deployments must not introduce degraded performance. This requirement almost by itself should be enough to justify the expense of a full GRID architecture as the underlying infrastructure of the SOA. We should not assume that an SOA will be performance scaleable in mission critical environments without a GRID.**
  - **No single points of failure can be tolerated. Simply stated, a break in any software component at any level will cause the service to be unavailable if HA/DR technologies are not implemented.**

- **Conclusion: a standalone SOA will be insufficient in terms of providing infrastructure stability. I am proposing that a highly available, disaster recoverable, GRID model (overlain with availability and performance monitoring agents) be implemented in order to sufficiently cover the reliability, performance, and availability issues needed for combat missions. A GRID infrastructure, with HA/DR monitoring of all components including the services and their sources themselves, should be selected to achieve this level of quality and availability.**

GRID Model of Multiple Executing FNEPs with Agent Monitors - Each FNEP Representing a Lenahan QoS Scale Value of 7 – Which means that all selected services in all architecture levels must be tagged as to HA/DR & GRID Compliance
(Modified from Original NASA Graphic)

FNEP 3 HA/DR Primary

FNEP 3 Composed UDOP Model With Choreography

FNEP 3 -HA Monitoring Agents

FNEP 3 HA/DR Secondary

FNEP 1 HA/DR Primary

Hypothetical Composite Operational Picture (per JL not real)

Virtual Global Air Space

FNEP 2 HA/DR Primary

FNEP 1 HA/DR Secondary

FNEP 1 -HA Monitoring Agents

FNEP 2 HA/DR Secondary

Composed Search & Rescue Model With Choreography

SAN Location A

SAN Location B

FNEP 2 -HA Monitoring Agents

Composed Force Positioning Model With Choreography

FNEP 1 Search & Rescue

HA/DR Storage Area Network

- Ops Data
- Weather Data
- Drone Schedule Data
- Terrain Data
- Surface Data
- Sub Surface Data
- Radar Tracks
- Sonar Tracks
- Digital Flight Data

FNEP 2 Create Force Positioning